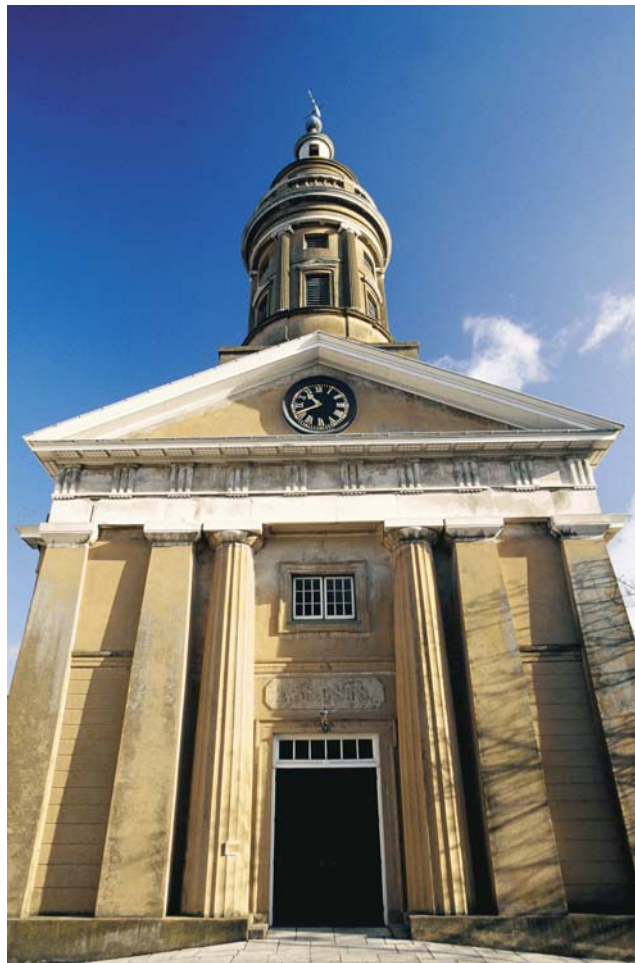


BAILIWICK OF GUERNSEY



DATA PROTECTION COMMISSIONER REPORT FOR 2006



MISSION STATEMENT

The Data Protection Office will encourage respect for the private lives of individuals by:

- *promoting good information handling practice,*
- *enforcing data protection legislation and*
- *seeking to influence national and international thinking on privacy issues.*

CONTENTS

FOREWORD	2
DATA PROTECTION LEGISLATION	3
Rehabilitation of Offenders.....	3
Amendments to the Law	4
DATA PROTECTION ISSUES	5
Credit Reference Agencies	5
Identity Theft	5
Identity Cards.....	5
Notification of Security Breaches.....	6
Transmission of SWIFT Data to the US	6
NOTIFICATION	8
Register Entries.....	8
Internet Statistics.....	9
Notifications by Sector	10
Exemptions	10
Payment and communications methods.....	11
Security Statements.....	13
STAFFING AND STAFF DEVELOPMENT	14
RAISING AWARENESS.....	15
Delivering presentations and training.....	15
Involvement in Working Groups	15
Making use of the media.....	15
Guidance Notes Published by the Commissioner.....	16
Developing the Internet Web Site.....	18
Registrations with the Preference Services.....	19
ENFORCEMENT	20
Notices	20
Complaints	20
Case Studies	23
International Conference of Data Protection Authorities	30
European Spring Conference	33
International Working Group on Data Protection in Telecommunications (IWGDPT).....	33
Liaison between the British, Irish and Islands' Data Protection Authorities.....	34
Liaison with the UK Government.....	35
Data Protection Forum.....	35
Information Privacy Expert Panel.....	35
OBJECTIVES FOR 2007	36
FINANCIAL REPORT.....	38
APPENDIX.....	40

FOREWORD

This is my sixth annual report to the States and the first covering my second term of office as Data Protection Commissioner for the Bailiwick of Guernsey.

During the year, the States approved a number of enhancements to the Data Protection legislation and an increase in Notification fees, which it is anticipated will come into effect during 2007.

The Rehabilitation of Offenders Law came into force in July. This Law limits the circumstances under which someone's spent convictions may be disclosed and, following an extensive period of consultation which had commenced in 2003, I issued a Code of Practice which specified the circumstances under which various categories of conviction and intelligence information could be disclosed in connection with employment and voluntary work.


The first prosecution in Guernsey that included allegations of Data Protection offences commenced in December 2006 and concluded in January 2007. One of the allegations was proven and the offender was fined. However, I am pleased to report that it was not necessary to serve any Enforcement Notices or Information Notices during 2006.

My office continues to receive numerous calls for advice from both individuals and businesses and we have continued the practice of giving short training courses to small groups of staff on request. Further guidance notes were issued and published on the website, which continued to be a popular way for people to obtain information.

We also received a number of requests for more detailed information about our activities and accordingly a Transparency Policy, concerning the disclosure of information held by the Office about individuals and organisations, was published.

Expenditure remained under control and income from notifications continued to rise, such that the overall cost of the office to the taxpayer reduced slightly in 2006. If the planned increase in fees comes into effect during the coming year, I would anticipate a further reduction in net cost in 2007.

The Guernsey Office will be organising one conference and hosting two international meetings of Data Protection authorities during 2007. These events help to ensure that the Office remains up to date with international developments and serve to reinforce the reputation of the Bailiwick as a well regulated jurisdiction that is ideally suited to the conduct of international business.

A handwritten signature in black ink, appearing to read "Peter Hamel", is written over a horizontal line.

Data Protection Commissioner, April 2007.

DATA PROTECTION LEGISLATION

Rehabilitation of Offenders

The Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 (Commencement, Exclusions and Exceptions) Ordinance came into effect on 1st July 2006. This legislation provides that anyone who may have been convicted many years ago of relatively minor offences is normally deemed to be rehabilitated and is able to have a 'clean slate'.

Although not ostensibly Data Protection legislation, there are significant Data Protection ramifications in that the Rehabilitation of Offenders legislation makes it an offence for spent convictions to be disclosed other than in defined circumstances; consequently, the Commissioner issued a Code of Practice under section 51 of the Data Protection Law that specified in more detail how the Rehabilitation of Offenders and Data Protection legislation should be interpreted in the context of employment

Section 56 of the Data Protection Law criminalises the practice of "enforced subject access" whereby an employer might require an employee or potential employee to obtain and then disclose a list of their previous convictions. It is anticipated that this section will be commenced in 2007.

Three guidance notes were published, corresponding to the three parts of the Code of Practice, directed towards:

- individuals,
- employers and
- the police disclosure unit.

Three categories of disclosure were identified:

- Basic Disclosures, which are available to all employers:
- Standard Disclosures, which include spent convictions, available to a limited set of employers; and
- Enhanced Disclosures, which include spent convictions and intelligence information, available only for specified categories of employment or voluntary work with children or vulnerable adults.

Training courses and presentations were given throughout the year, building on the consultation process that had commenced originally in 2003 and the Office responded to numerous queries as to the effect of this new legislation and the Code of Practice in particular circumstances.

Amendments to the Law

At the meeting on 27th September 2006 the States approved proposed amendments to the Data Protection legislation as detailed in a letter from the Home Department dated 25th July 2006¹. The proposals were:

1. Following the commencement of the Rehabilitation of Offenders (Bailiwick of Guernsey) Law, 2002 on 1 July 2006, it is recommended that section 56 [enforced subject access] is brought into force and the Law is amended to include a definition of what constitutes a relevant record in section 56(5) so as to exclude a Disclosure issued by or on behalf of the Chief Officer of Police in accordance with any code of practice issued by the Commissioner under section 51(3) of the Law;
2. That section 54(3) [co-operation with the EU] of the Data Protection Law is brought into force;
3. That section 62 [application to the States and the Crown] is amended, as proposed by the Commissioner but subject to the qualification, insofar as the Crown is concerned, raised by Her Majesty's Procureur and described in paragraph 4 of this report;
4. That Section 43(1) [serving of a notice on any organisation] of the Law is amended, as proposed, and that an equivalent amendment is made to paragraph 4 of Schedule 1 to the Privacy and Electronic Communications regulations;
5. That the Law be amended to correct the small omissions and oversights identified and to create statutory immunity for the holder of the Office of Commissioner and certain persons acting for him with his authority;
6. That the fee for a notification or renewal of a notification be increased to £50, except in the case of not for profit organisations, where no fee will be payable.

It is anticipated that the legislation implementing these Resolutions will be enacted during 2007.

It is understood that the European Union may be considering enforcement action against the United Kingdom with regard to its transposition of the Data Protection Directive. If that action is successful there may be the need for consequential amendments to the UK legislation.

The States will be advised in due course if in the Commissioner's view any matching amendments to the Bailiwick legislation might be recommended in order to ensure the continued adequacy of the local Data Protection régime.

¹ Billet d'État XVI, September 2006 p. 1660

DATA PROTECTION ISSUES

Credit Reference Agencies

Some Guernsey residents have reported difficulty in obtaining goods and services if such provision involves the use of the UK-based credit reference agencies (such as Experian, Equifax and Call Credit).

This is because a major element in a credit score is a reference to the UK electoral roll to confirm the name and address details of the applicant.

Guernsey residents do not appear on the UK electoral roll and the Guernsey electoral roll is not published or made available other than for election purposes.

However, following talks with the Deputy Registrar General of Electors (Electoral Roll), and the Home Department, that Department has agreed to issue certificates to anyone who is on the electoral roll and needs to provide evidence of residence for credit reference purposes. The three major UK credit reference agencies have undertaken to accept these certificates as evidence of residence.

The Commissioner welcomes this initiative, which should enable those residents who are on the electoral roll to have easier access to credit facilities in future.

Identity Theft

During the year there were some well-publicised incidents of identity theft concerning UK residents.

13,000 employees of the Department of Work and Pensions and of Network Rail had their identities stolen and used to make fraudulent claims for tax credits.

Twenty UK customers of HSBC were said to have suffered financial loss after a leakage of personal data from the bank's Indian data centre.

The Financial Services Authority was called in to investigate the circumstances surrounding the theft of a laptop belonging to an employee of Nationwide Building Society that contained confidential information about customers' accounts. The FSA found that the Building Society did not have adequate security measures and imposed a fine of £980,000. This is a much greater penalty than would normally be available under Data Protection legislation.

Identity Cards

Following much public criticism of its original proposals, the UK Government abandoned plans to create a National Identity Register from scratch, but instead proposed to use existing sources such as the National Insurance database, Passport Agency database and Drivers' database to underpin the proposed identity cards system.

It remains to be seen how the Government manages to address the errors and inconsistencies which undoubtedly will be found between these various sources of data.

The UK Government also emphasised that it was not intended to store any health information on the identity card system, but questions were raised as to the extent of data sharing between government departments and agencies that might result from the adoption of this system.

The report on Service Transformation by Sir David Varney² that was published in December 2006 certainly envisaged a much greater level of data sharing in order to improve the level of service delivered to the citizen.

There is undoubted concern that this proposed increase data sharing might compromise individual privacy.

Notification of Security Breaches

The European Commission published proposals for an amendment to the Privacy Directive 2002/58/EC which would require providers of electronic communications networks to notify customers and regulators of any breaches of security that might result in personal data being made available to others.

This proposal went beyond the existing requirement that subscribers be informed of any risks to security and the measures that should be taken to guard against such risks.

Critics pointed out that a similar requirement already existed in California and 33 US States and had resulted in a flood of notifications to consumers and a consequential erosion of consumer confidence in conducting internet transactions.

Other commentators suggested that the proposed requirement did not go far enough and that other service providers, such as those providing financial services should be placed under a similar obligation.

Transmission of SWIFT Data to the US

In June, the Commissioner, in common with other European Commissioners, received a circular letter by email from Privacy International. A copy of that letter is shown below.

The Commissioner was concerned to hear of this problem, but was aware that the European Commissioners, in particular the Belgian Commissioner, was investigating this matter fully and felt that there was little that he could add to the process, as the alleged disclosures were essentially being made on the authority of the Belgian Office of SWIFT.

Subsequently, it was reported that the Belgian Office of SWIFT had contended that it was operating within the law as it had audited the subpoenas for information from the US and had come to an agreement that only those records concerned with alleged counter terrorism would be disclosed.

Despite these assurances, the Article 29 Group of European Commissioners delivered an adverse opinion on this matter³ and the European Data Protection Supervisor concluded⁴

² Service Transformation – A better service for citizens and businesses, a better deal for the taxpayer, http://www.hm-treasury.gov.uk/pre_budget_report/prebud_pbr06/other_docs/prebud_pbr06_varney.cfm

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf

that the secrecy surrounding the transfers to the US was regrettable and recommended that the European Central Bank promoted solutions to bring compliance within Data Protection rules within the oversight by the ECB of the SWIFT system.

Dear Commissioner **Harris**,

Complaint: Transfer of personal data from SWIFT to the U.S. Government

I am writing with regard to recently publicised activities of the Society for Worldwide Inter-bank Financial Telecommunications (SWIFT) involving the covert disclosure of personal information relating to residents of Guernsey.

This disclosure of data has been undertaken ostensibly on the grounds of counter-terrorism. The disclosures involve the mass transfer of data from the SWIFT centre in Belgium to the United States, and possibly direct access by U.S. authorities both to data held within Belgium and data residing in SWIFT centres worldwide.

It appears that the activity was undertaken without regard to legal process under Data Protection provisions, and it is possible that the disclosures were made without any legal basis or authority whatever. In all cases the disclosures were made without the knowledge or consent of the individuals to whom the data related. To the best of our knowledge, the disclosure activity is ongoing.

The scale of the operation, involving millions of records, places this disclosure in the realm of a fishing exercise rather than legally authorised investigation.

At this stage we do not have enough information to determine how many of Guernsey's residents have been the subject of these disclosures, but there is a probability that the SWIFT activities involve mass disclosure.

The office of Belgium's Prime Minister confirmed that: "the cooperative (SWIFT) had received broad administrative subpoenas for millions of records".

An "administrative subpoena" takes the form of a letter issued without judicial authority.

We are also concerned that this data could be used by US authorities for a range of non-terrorist related activities. As this information can amount to a profile of all financial transfers over periods of years the additional uses could vary widely to include taxation monitoring and even espionage.

We are concerned that the practice substantially violates Data Protection law and we request that your office institutes an investigation without delay.

We also ask that you intervene on behalf of Guernsey's residents to seek the immediate suspension of the disclosure programme pending legal review.

Privacy International

⁴http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2007/EDPS-2007-1-EN_SWIFT.pdf

NOTIFICATION

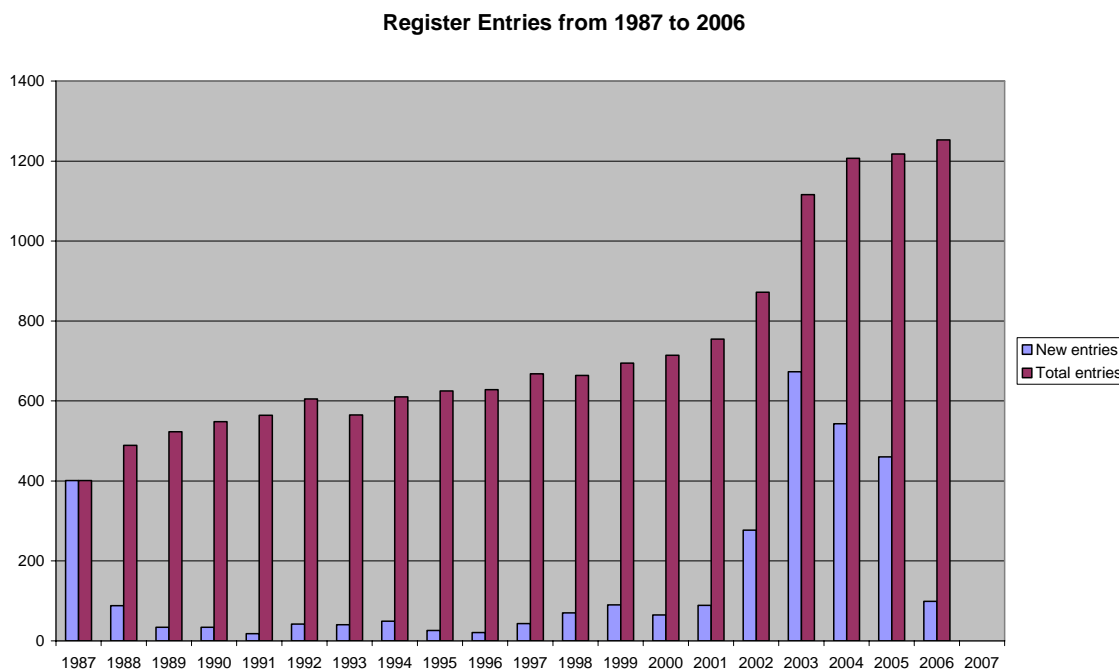
Section 17 of the Law requires Data Controllers to “Notify” the Commissioner of their processing of personal data. This Notification is on an annually renewable basis and covers all processing that is not exempt.

Exemptions from Notification exist for manual data, certain charitable and not-for-profit organisations and for the processing of data associated with the core business purposes of accounts, staff administration and marketing.

The annual fee for Notification was set in 2002 as £35, but in 2006 the States resolved that this fee should increase to £50 and it is anticipated that the legislation enabling this change will be enacted during 2007. At the same time, those charitable organisations which are exempt from the requirement to Notify will be able to Notify free of charge.

Register Entries

The chart below illustrates the rise in register entries since Registration under the original 1986 Law commenced in October, 1987. As noted in last year's report, the number of Notification entries appears to have stabilised at around 1250.



By the end of December 2006, there were 1253 Notifications on the register, whilst a total of 791 Registrations and 146 Notifications had been closed since 2002.

There were 99 new Notifications in 2006 and 65 closures - a net increase of 34, whilst in the peak year in 2003 there had been over ten times that activity, with 673 new Notifications and 227 closures – a net increase of 446.

Internet Statistics

The Notification process may be completed online at <http://www.dpr.gov.gg>.

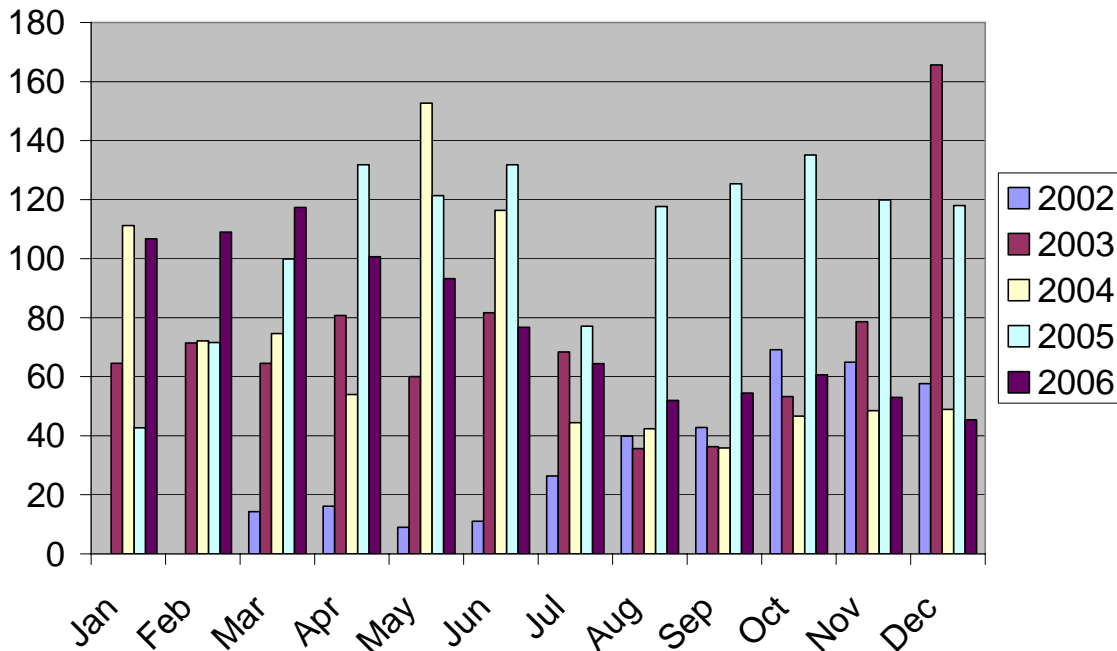
This site is used both by those wishing to create and maintain their own Notification entries and by the staff of the Data Protection Office.

Statistics gathered over the past three years show that approximately 38% of the Notification site accesses were for downloads of manuals and information, 20% for administration purposes and the remainder (42%) for online notification activities.

The chart below shows the variation in the average daily activity on the online Notification site between the commencement of Notification in 2002 and December 2006; the vertical axis represents the average daily rate of successful requests for pages of data from the site each month.

The variations in activity generally correspond with variations in the volume of new Notifications and renewals that are dealt with each month and have stabilised at a lower level, following the expiry and subsequent re-notification of all the Registrations under the 1986 Law that took place between 2002 and 2005.

Notification Site Activity between 2002 and 2006

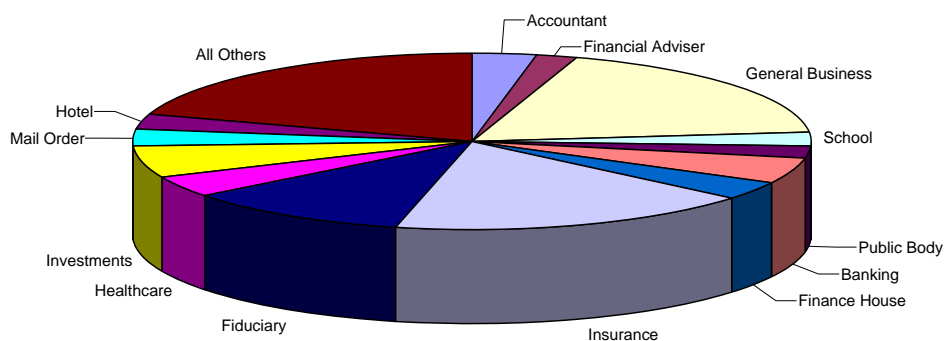


Notifications by Sector

The Notification process requires data controllers to indicate the nature of their business activity. This requirement not only simplifies the process, as it allows for the generation of a standardised draft Notification based on a template, but also enables an indicative record to be maintained of the number of Notifications by industry sector.

The chart depicted below shows the cumulated distribution of notifications at the end of 2006 by industry sector, continuing a similar pattern to that of previous years.

Notifications by sector in 2006



The largest proportion of Notifications used a General Business template (18%), which clearly had the effect of skewing the detailed statistics to some extent; however, the remaining proportions were: Insurance (17%), Fiduciary (11%), Investments (6%), Banking (5%), Healthcare (4%), Mail Order and Finance House (both 3%), schools public bodies and financial advisers (2%), with 'All Others' [covering some 40 other classifications] being 20%.

Exemptions

Exemptions from the need to Notify may be claimed by those whose processing is limited to the core business purposes of accounts & records, staff administration and a limited amount of marketing to existing clients.

An exemption is also available to most voluntary organisations, charities and to those whose processing is limited to manual data. However, once CCTV is used by an organisation for the prevention and detection of crime, these exemptions from Notification are lost.

Organisations that are exempt may choose to Notify voluntarily, thereby relieving themselves of a responsibility to provide information on request under section 24 of the Law. The number of voluntary Notifications fell by 8 to 39, (3% of the total).

In 2003, the Data Protection Office commenced the compilation of a list of those organisations that had informed the Commissioner that they were exempt from Notification and by the end of that year 303 organisations were so listed. The exempt list was primarily designed to assist in monitoring compliance and to avoid pestering those who had previously advised the Office that they were exempt.

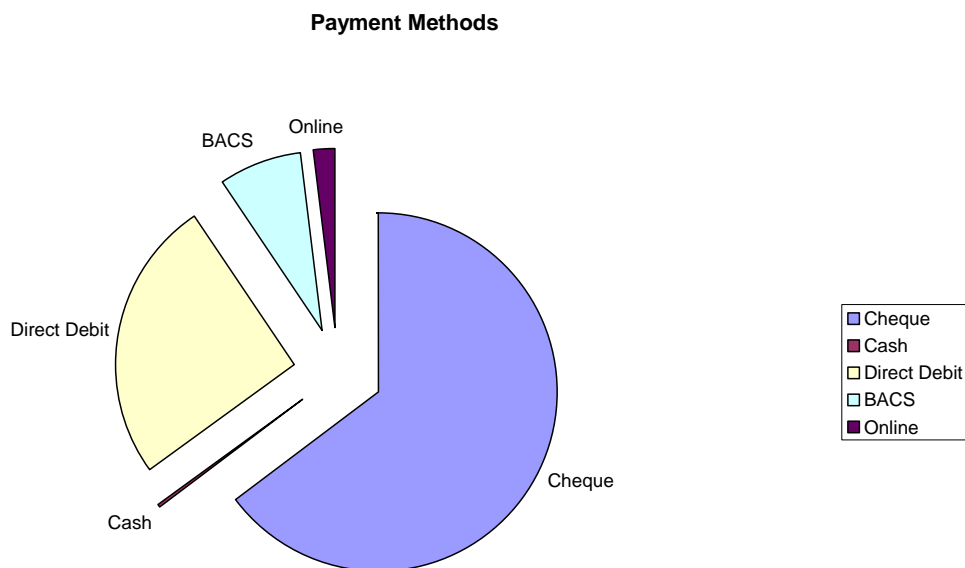
During 2004, the exempt total rose to 447; in 2005, it fell to 441 and in 2006, the number of exempt organisations rose slightly to 446. This represents 26% of the overall total [of 1699 exempt and notified organisations].

Payment and communications methods

Renewal reminders issued during 2006 advised data controllers of the introduction of alternative means for the payment of fees.

The number paying by these various means in 2006 was as follows:

Payment methods for Data Protection fees		
Cheque:	803 (65%)	Online: 24 (2%) BACS: 95 (8%)
Direct Debit:	317 (26%)	Cash: 4 (0.3%)



During 2005, 286 (23%) of the fees were paid by annual Direct Debit, so this method of payment continues to show a small increase. BACS and Online methods had not been promoted until 2006, so it remains to be seen whether they become more popular.

1069 organisations (85%) provided an email address for communication purposes; this was used for the issue of automatic renewal reminders to those who did not renew by Direct Debit; of those, just 179 required a second reminder to be sent by post. There were 22 second reminders issued to organisations whose first reminder had been sent by post. It was necessary to resort to final reminders in 37 cases and this resulted in some payments being overdue. It appears that some data controllers do habitually ignore final reminders resulting in the need for follow-up action. Although in 2006 no referrals were made to the Police, a significant amount of administrative time was spent on pursuing these late payers and it is recommended that a financial penalty should be imposed in the case of those who are late in renewing their notifications.

The most common reason for second and final reminders was that the data controller's address or the email address of the administrative contact had changed since Notification. Data controllers were reminded that it is an offence for an organisation to fail to keep its registration particulars up to date.

Nevertheless, the use of automated email reminders and Direct Debits continues to reduce substantially the administrative effort involved in the Notification process.

Security Statements

Part 2 of the Notification Form includes a security statement, in which data controllers are required to answer a number of questions related to their information security policy and provisions; the answers given were as follows:

Security Survey Answers	
Do your security provisions include:	YES
Adopting an information security policy?	86%
Taking steps to control physical security?	94%
Putting in place controls on the access to information?	90%
Establishing a business continuity plan?	89%
Training staff on security procedures?	83%
Detecting and investigating breaches of security?	85%
Adopting British Standard 7799 (ISO 9001)?	12%

These answers show that, in general, security is taken seriously by the overwhelming majority of organisations, but that the fairly onerous British Standard has been adopted by only a small minority of organisations.

STAFFING AND STAFF DEVELOPMENT

Since its inception, the Office of the Data Protection Commissioner has comprised three people: the Commissioner and Assistant Commissioner, both of whom work full time and the Personal Assistant to the Commissioner, who works part-time.

The Commissioner is a statutory public appointment, but members of his staff are seconded from the Home Department of the Civil Service and are wholly responsible to him.

The Assistant Commissioner devotes the majority of her time to compliance activities, responding to enquiries from individuals and organisations and running training courses for the public and private sector.

The Personal Assistant undertakes all of the administrative activities for the office including the processing of Notifications and the reconciliation of the accounts.

The Commissioner remains of the view that, whilst his office remains responsible only for the Data Protection Law and the associated Privacy Regulations, the current establishment of one full time Assistant and one part time Personal Assistant represents a satisfactory minimum level of staffing resource, which enables him to discharge his responsibilities adequately under the Law.

The use of external consultancy has been limited to the provision of expert legal advice and for assistance in the planning of the international conferences.

The Commissioner is keen to encourage the academic, technical, administrative and professional development of his staff and to that end supports their attendance at training courses and relevant conferences and other forms of personal development.

The Commissioner remains a member of the E-commerce and IT Advisory Group of the GTA University Centre and of the Guernsey Digimap Management Board and attends relevant seminars and workshops organised by the GTA University Centre and the Guernsey International Section of the British Computer Society.

The Assistant Commissioner has attended some GTA seminars, participated in the UK Data Protection Forum and continued her legal studies with the Open University. She also furthered her knowledge by attending seminars in the UK organised by the Direct Marketing Association, White & Case and 'Data Protection Law and Policy'.

During 2006, the Personal Assistant enhanced her training by attending a specialised course run by the GTA University Centre dealing with the management of email.

RAISING AWARENESS

There is a continual need to ensure that individuals are made aware of their rights under the Law and organisations that process personal data are made aware of their responsibilities.

The Awareness campaign for 2006 has included the following activities:-

- Delivering presentations and training
- Involvement in working groups
- Making use of the media.
- Giving compliance advice
- Developing the Internet web site

In addition, the Office has assisted in sourcing the provision of external training specialists for a number of organisations.

Delivering presentations and training

The Commissioner and Assistant Commissioner delivered a total 26 talks and presentations throughout the year to many professional associations and organisations in the public and private sectors. These included: schools, nursing homes, finance institutions, law firms, retail businesses and voluntary organisations.

The total audience reached in this way was around 358, compared to 916 in 2005.

The GTA ran a local course leading to the award of the ISEB Certificate in Data Protection. Three students graduated successfully from this course. The provision of further courses will be subject to demand and budgetary considerations.

Involvement in Working Groups

The Commissioner and Assistant Commissioner participated in the States Data Guardians Group. The activities of the group have initially been involved with the establishment of data sharing protocols between various departments and sections within the government.

Making use of the media

28 articles or letters relating to Data Protection were published in the local media during 2006, (compared with 15 in 2005) covering topics such as:

- The ISEB Data Protection qualification;
- ID cards;
- Rehabilitation of Offenders law;
- The Annual Report;
- Proposed amendments to the Data Protection legislation;
- The re-appointment of the Commissioner;
- Prosecution for alleged offences under section 55 of the Law;

- Disclosure and retention of credit card numbers by merchants;
- A disciplinary case in the UK foundering on alleged incompatibility of Law;
- Use of CCTV in reports of criminal activity
- The issue of new Guidance Notes.

Guidance Notes Published by the Commissioner

The number of Guidance Notes published by the Commissioner during the year rose to **29**, compared with 23 in 2005.

The new publications, which were produced in printed form and also made available for download from the web site, were:-

- Three Guidance notes on the Rehabilitation of Offenders legislation
- Transparency policy
- Work references
- Marketing guidance for businesses.

A full list of available publications is given overleaf.

Approximately 905 hard copies of the literature were distributed to individuals and organisations during 2006, compared with 1664 copies in 2005.

It is not currently practical to estimate the number of electronic copies of these guidance notes that were viewed or downloaded from the website.

Guidance Notes published by the Data Protection Office

Baby Mailing Preference Service: <i>How to stop the receipt of unwanted mail about baby products</i>
Be Open...with the way you handle information: <i>How to obtain information fairly and lawfully</i>
CCTV Guidance and Checklist <i>Explains how to comply with the law in relation to the use of CCTV</i>
Charities / Not-for-Profit Organisations
Data Controllers: <i>How to comply with the rules of good information handling</i>
Dealing with Subject Access Requests
Disclosures of vehicle keeper details <i>Explains when vehicle keeper details can be disclosed</i>
Exporting Personal Data
Financial Institutions
Mail, telephone, fax and e-mail preference service <i>How to stop the receipt of unsolicited messages.</i>
Marketing – A Guidance for Businesses
No Credit: <i>How to find out what credit references agencies hold about you and how you can correct mistakes</i>
Notification – a Simple Guide
Notification – a Full Guide
Notification Exemptions
Personal Data & Filing Systems (guidance on what makes information “personal” and explains what manual records are covered by the Law)
Privacy Statements on Websites – a Guidance
Respecting the Privacy of Telephone Subscribers
Recommended Disclosure Policy for the Central Records Office Of Guernsey Police
Rehabilitation of Offenders – Guidance for applicants – Police Disclosures
Code of Practice & Explanatory Guide – Disclosure of Criminal Convictions in connection with employment
The Data Protection Law and You: <i>A Guide for Small Businesses</i>
Spam – How to deal with spam
States Departments – a Guidance
Transparency Policy
Trusts and Wills – a Guidance
Violent warning markers: use in the public sector <i>How to achieve data protection compliance in setting up and maintaining databases of potentially violent persons</i>
Work References
Your rights under the Law: A Guidance for Individuals

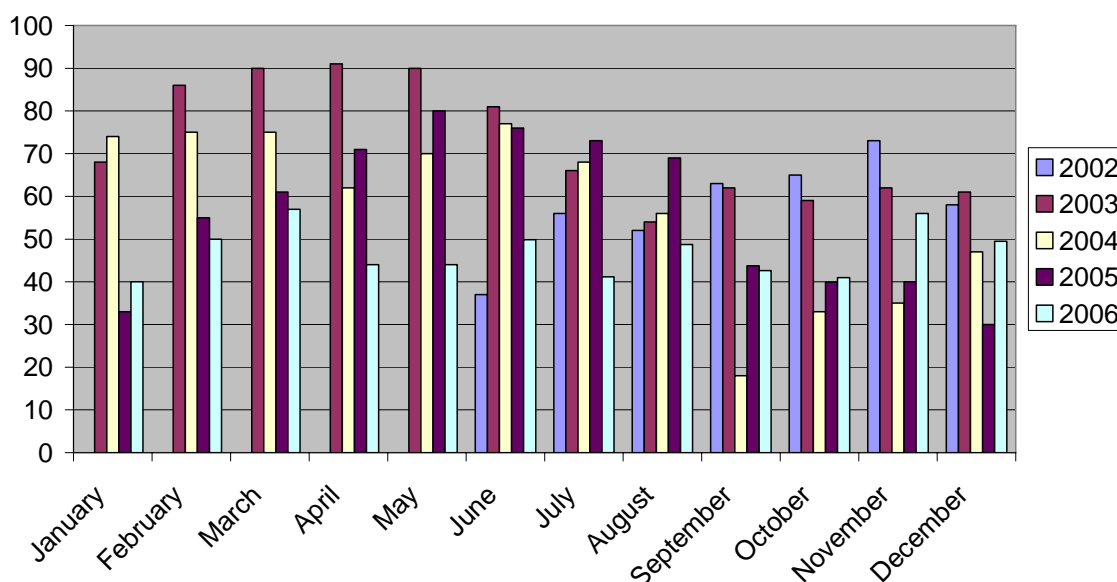
Developing the Internet Web Site

Work continued throughout the year to keep the information on the website: <http://www.gov.gg/dataprotection> up to date.

A chart of the average number of pages viewed per day between October 2004 and December 2006 is shown below. Currently, it would appear that about 50 pages per day are being accessed, compared with a peak of 90 pages per day in 2003; the most popular pages continuing to be those containing Guidance Notes.

It is reasonable to presume that the provision of ready access to information on the web site has reduced need for many people to make routine enquiries for information from the Data Protection Office. It is evident that many people who do call the office for advice have already obtained basic information by first consulting the Internet web site.

Average Daily Visits to Internet Site



It was noticed that the number of referrals from the old website: www.dataprotection.gov.gg continued at a reasonably high level throughout the year, so it was clear that many users had that old URL still saved in their browsers. There are no plans at present to discontinue that URL, although the underlying information on the web pages will be removed as it is has not been updated since the transfer and so is now over two years out of date.

Registrations with the Preference Services

The Preference Services are administered by the Direct Marketing Association of behalf of Ofcom, the UK telecommunications regulator. The scope of the Preference Services covers the British Isles Integrated telephone numbering scheme and the Royal Mail Postcode areas, of which the Channel Islands and the Isle of Man are part.

The Telephone Preference Service, TPS, allows individuals to opt-out of the receipt of unsolicited marketing calls. Although the regulations covering the TPS apply only to marketing organisations based in the British Isles, in practice TPS registration appears to reduce but not eliminate the receipt of calls originating from overseas, as many reputable overseas telemarketers appear to screen their calls against the TPS database.

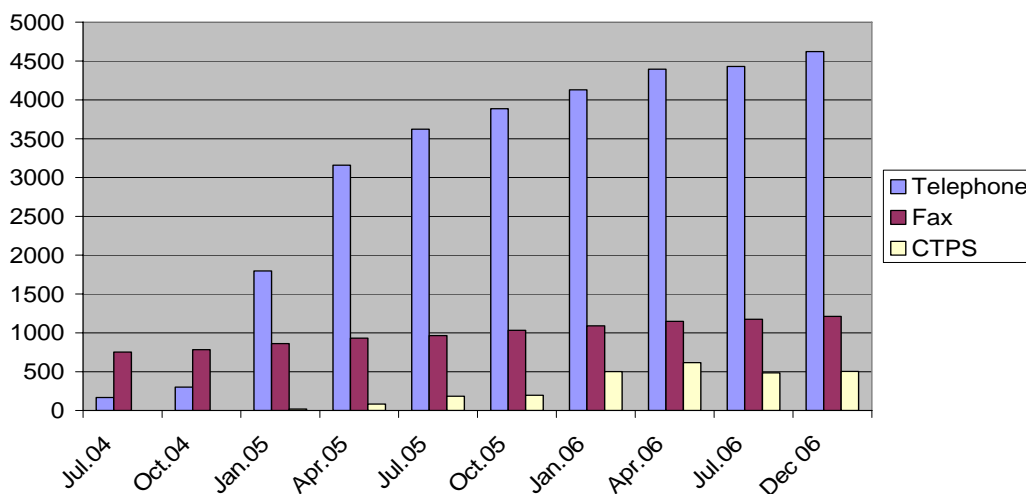
The Fax Preference Service, FPS, allows any individual or business with a fax machine to opt out of the receipt of unsolicited marketing faxes whereas the Corporate Telephone Preference Service, CTPS, is for use by organisations wishing to opt out of the receipt of marketing calls.

The Preference Services were initially promoted in Guernsey by the Office in 2004, following a number of complaints about marketing calls and a service was offered whereby the Office undertook the registration on behalf of local residents. The services are now advertised within the information pages at the front of the Cable & Wireless and Wave Telecom directories.

The chart below shows that registrations for TPS continue to show an increase, with over 4,500 numbers being registered, compared with around 4,000 at the end of 2005. Only 10% of those registrations were initially made by the Data Protection Office, which shows that the vast majority of people are now confident to register for themselves.

Registrations for FPS remain fairly static and those for CTPS have fallen slightly, possibly because this service is annually renewable and some businesses may have failed to realise this.

Registrations for Preference Services



ENFORCEMENT

The Law provides for a number of offences:-

- a) Failure to notify or to notify changes to an entry;
- b) Unauthorised disclosure of data, selling of data or obtaining of data;
- c) Failure to comply with a Notice issued by the Commissioner.

The Commissioner may serve an Enforcement Notice where he has assessed that a controller is not complying with the principles or an Information Notice where he needs more information in order to complete an assessment. With the advent of the Privacy in Electronic Communications Regulations, the Commissioner's power to issue Notices has been expanded to cover non-compliance with those Regulations.

Notices

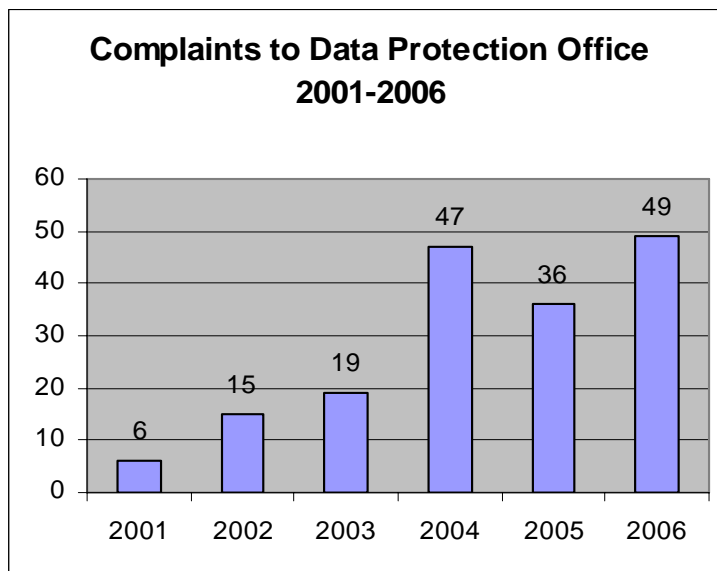
One data controller was served with a preliminary Information Notice, but no Information Notices were issued in 2006, compared with the 2 data controllers who were served with Information Notices in 2005.

No Enforcement Notices were issued in 2006, whereas in 2005, 2 data controllers were served with Enforcement Notices relating to email marketing.

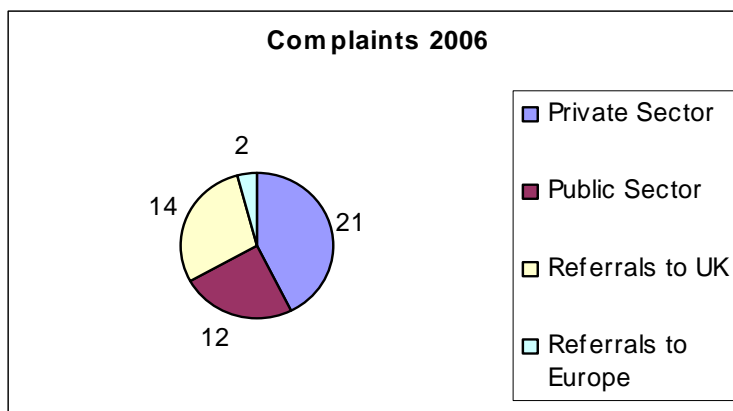
Complaints

There were a total of 49 complaints received by the Commissioner during 2006, compared with 36 in 2005 and 47 in 2004.

A relatively smaller number of complaints were processed in prior years, as is shown opposite.



The breakdown of complaints received in 2006 and depicted opposite, shows that 21 related to the private sector and 12 to the public sector. There were 14 complaints referred to the UK and of the 2 referred to Europe, 1 was to Denmark and 1 to Hungary.



The referral to Denmark was made because a Danish company that utilised a fulfilment house in Guernsey had presented inaccurate data in respect of a client in a UK national magazine. The Danish Data Protection Authority referred this complaint to the national authority with the relevant remit.

The complaint to Hungary was made by Guernsey's Assistant Data Protection Commissioner. The substance of this complaint was that her personal data were disclosed to another passenger at the border control on entering Budapest. The passenger was instructed to compare his passport with that of the Assistant Commissioner. The Assistant Commissioner reported this incident to the Hungarian Commissioner, the host of the conference she was attending.

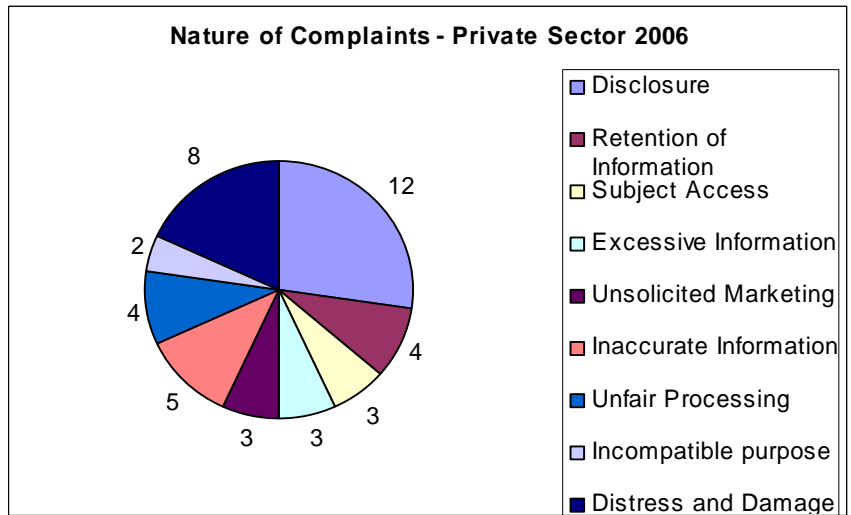
An investigation was conducted and it was found that correct procedure had not been followed. The incident was dealt with in the course of a "commander class" on a training day and was built into the training material.

Also in line with the recommendations of the Hungarian Commissioner, the National Commander of the Hungarian Border Guards took the following measures:-

- 1. The Ministry of Foreign Affairs for the Republic of Hungary was requested to obtain a passport sample of Guernsey together with samples of passports of Jersey and the Isle of Man. These were to be included in the passport sample and security features database (Document) of the Hungarian Border Guards.*
- 2. A position has been issued that citizens of Guernsey shall qualify as citizens of beneficiary countries; this means they shall go through only minimum control as opposed to the more rigorous basic control when entering Hungary.*

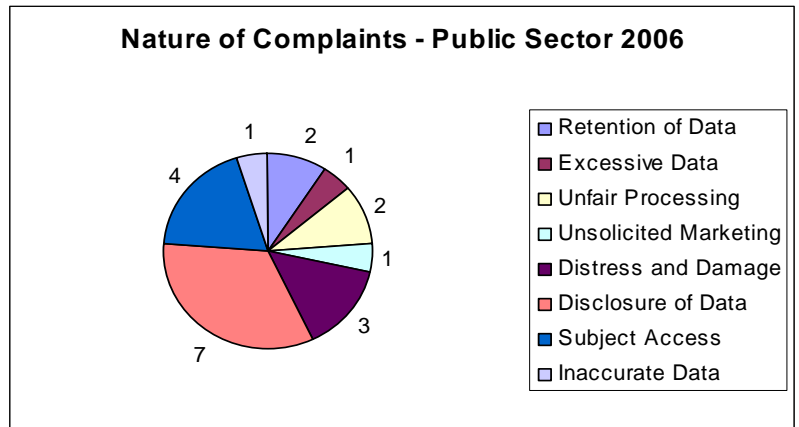
The Hungarian Commissioner was confident that implementation of these measures should prevent any further problems for Bailiwick residents entering Hungary.

A breakdown of the 21 complaints against the private sector can be seen opposite. A complaint may involve an alleged breach of one or more of the data protection principles. For instance an inappropriate disclosure of information may not only be a breach of security but could also be construed as unfair processing, i.e. using the personal information of a person without informing them that you will do this.

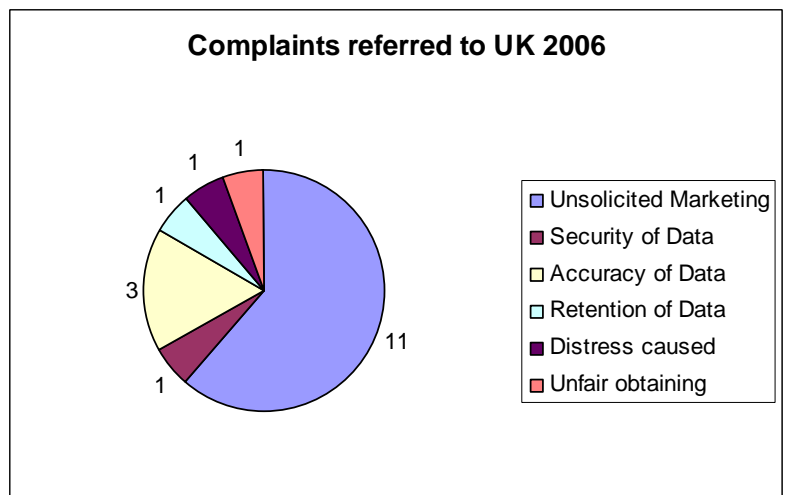


This may also have the effect of causing damage and distress. Likewise, damage and distress may also be caused if information is recorded inaccurately or used for a purpose which was not communicated to the individual at the time of collecting the information.

The 12 complaints made against the public sector mainly involved allegations of breaches involving disclosure of information and denying individuals right of access to their own information. Cases of alleged inaccurate processing and unnecessary retention of information were also included.



Of the 14 complaints referred to the UK Commissioner, 11 involved unsolicited marketing, 3 involved the inaccurate processing of data, with the remainder on data security, unnecessary retention of data, unfair obtaining of information and causing distress through the processing of data.



Case Studies

A selection of these complaints is detailed below.

Case Study 1

An individual complained that her landlord had disclosed her personal information, namely her work telephone number, to a third party, a contractor without her consent.

The contractor contacted her to arrange a time to access her property in order to carry out a repair.

The Tenants' Handbook stated that when reporting a repair tenants are required to give a daytime telephone number; it also stated "for internal repairs, we will arrange for a contractor to contact you to make an appointment".

The tenant had given her work telephone number as the daytime contact number.

Accordingly, the Commissioner was of the opinion that no unauthorised disclosure was made by the landlord. The tenant had been made aware through the Handbook that a contractor would make direct contact.

There was no breach of the first data protection principle; this principle states that personal information must be processed fairly and lawfully. The landlord was being fair in informing the tenant that she would be contacted by the contractor. The tenant had provided her work telephone number when reporting the fault thus implying that she consented to being contacted by the contractor. The disclosure of the telephone number to the contractor was fair and lawful in this case.

This complaint was resolved quickly and was of a relatively minor nature but a lesson can nevertheless be learned from it. The Commissioner would advise individuals that they should carefully read any information provided by any party, landlord or otherwise, with whom they enter into any agreement.

Case Study 2

An individual complained to the Commissioner that his request for an offence of over five years old to be deleted from his driving licence was refused.

The Rehabilitation of Offenders Law (ROO) is now in force within the Bailiwick and, in accordance with this law, an offence which incurred a fine and a driving suspension would be considered spent after five years.

The Data Protection Law states that personal data must be processed lawfully; this means that personal information must be processed in accordance with the requirements of other legislation.

This would imply that any conviction considered as spent under ROO should not appear on a driving licence.

Under ROO the time of an offence is calculated from the time when a sentence is imposed.

In investigating the complaint it was discovered that according to the Road Traffic Law 1987 (RTL) any driving endorsement / disqualification details remain on a person's driving licence until five years from the date that the disqualification ends.

Hence there would appear to be a conflict between the provisions in ROO and RTL.

The Commissioner was informed that case law in the UK upheld Road Traffic Act provisions over Rehabilitation of Offenders Act provisions.

However the UK Traffic Act was enacted after the UK ROO Act. In the Bailiwick ROO was enacted after RTL and normally, in the case of a conflict between statutes, the provisions of the later statute would prevail.

Whilst the Commissioner took no action in this case, he did suggest that political action would be desirable in order to resolve the apparent conflict between these two statutes.

Case Study 3

The 7th data protection principle states that: “*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*”

There have been a number of complaints from the public about alleged breaches of this principle which are described below:

a) A member of the public brought merchant copies of credit / debit card receipts to the Commissioner's office. He had found these lying in the road near some open disposal sacks outside a restaurant.

The full credit card number and expiry date were on these receipts.

The Commissioner asked for the restaurant concerned to explain what its usual procedure was in the processing of credit / debit card receipts.

While a sound procedure was usually followed there was an occasion when someone who did not usually work “in front of house” inadvertently put the receipts into a rubbish sack which was then presumably opened by a seagull. It was also stated that staff not aware of procedures are usually supervised.

While no further action was taken in this case the Commissioner warned that Enforcement action would be taken should a similar breach of the law happen in the future.

b) A person received another person's credit card along with his own from an automatic cash dispenser.

On investigation the bank stated that this was due to a one-off technical fault which had been rectified at the earliest opportunity.

The Commissioner advised that this incident would be kept on record and Enforcement action would be taken should a similar occurrence arise. The Financial Services Commission was also informed of the incident.

c) It is now a requirement that when credit / debit cards are used in non face to face transactions a security (CVV) number is requested. This is to make it more difficult for persons to obtain products and services by merely using the information recorded on credit / debit cards receipts. However while the Commissioner recognises the necessity for all organisations to ask for the CVV number he advises that, in the interest of security, CVV numbers should be recorded separately from other information and not retained for longer than is necessary for business purposes.

c(i) A complaint was received about a local business recording and retaining the CVV number with other information. The business reviewed its procedures and practices and established that it was possible to process the CVV number separately.

c(ii) There was a general enquiry about the legality of a local charity asking for CVV numbers on membership application forms. The collection of CVV numbers in this way would only apply to application forms which are posted. The charity concerned had a sound procedure in place for the secure storage and earliest possible disposal of the forms. In considering this and the nature of the charity and its resources the Commissioner concluded that the practice was acceptable as the CVV number was intended to validate transactions in non face-to-face environments, such as by post.

Case Study 4

The Data Protection Law applies to all marketing messages sent to individuals whatever medium is used. Under the Law individuals have the right not to be marketed by any organisation, they can inform marketers that they do not wish to receive any more communications and if this request is ignored a breach of the Law occurs.

The Privacy and Electronic Regulations apply to marketing by electronic means and give rights to both individuals and legal entities. Explicit consent must be obtained from an individual before any marketing emails are sent. In the case of a legal entity an initial communication may be sent without obtaining consent. However, all marketing emails sent to individuals and organisations must contain the identity of the sender and an unsubscribe facility must be provided within each message.

Complaints have been received from individuals that they continue to receive unsolicited marketing messages by email even though they may have unsubscribed from the mailing lists.

Frequently, it is mail order firms that are the focus of these complaints.

When these complaints are investigated a recurrent theme that emerges is the individual may have indeed unsubscribed but only from a single email address, despite having received emails addressed to more than one email address.

A mail order company cannot be expected to know that a particular individual may have more than one email address.

It is important that a recipient informs the sender of all email addresses that he or she has registered. Not to do so may result in the receipt of further unwanted messages.

Case Study 5

Two individuals shared a flat, one of whom complained to the Commissioner that her personal information had been disclosed by her landlady. It was further claimed that the landlady had accessed the information through her workplace. Such a disclosure would be considered an offence under section 55 of the Data Protection Law.

In her submission to the Commissioner the tenant provided a copy of the written complaint which had been signed by herself and her partner and sent to the landlady's employer. The tenant also enclosed a report containing the results of an investigation that had been carried out by the employer.

As the tenant considered this report was not clear on how the information came to be disclosed she asked the Commissioner to investigate her complaint further.

The information in question was of such a nature that it could only have been obtained through the landlady's workplace. The tenant claimed the disclosure resulted in an unwelcome outcome for her and her partner.

Detailed questions were therefore asked concerning the actual disclosure, whether or not the landlady had legitimate access to the information in the course of her employment and if access by company personnel to records was audited.

The employer responded to the effect that the company held no account in the name of the tenant who had complained. The account was in the name of her partner.

This meant that the complaint could not be continued as technically the company did not hold any personal information relating to the complainant.

The complainant was advised to ask her partner to resubmit the complaint. As this did not happen the complaint was closed.

The Commissioner would remind individuals that he can only investigate complaints against organisations if they are from individuals whose personal information is being processed by those organisations. Representatives may be nominated by those who are adversely affected by an organisation's data processing activities. In this case study investigation of the complaint might have been continued had the partner nominated the tenant to act for her.

Case Study 6

An employee requested a copy of the rules of his company's bonus scheme as well as a copy of the assessment of his entitlement to a bonus.

His request was refused and so he made a second request for the documents through an advocate. In its reply to the advocate the company stated that the employee had been fully informed of the details of the bonus scheme, the criteria for assessment and of his personal measurement against those criteria. The requested documents were considered internal and confidential to the company and so were further refused.

The employee then complained to the Commissioner.

The company was informed that if an organisation processes any individual's personal information then that individual has a legal right to have such information communicated to him in an intelligible form and be provided with a permanent copy of it. The copy need not be a copy *exactly as held* by the company as long as it is intelligible. The supply of all intelligible information would mean that the employee has fully explained to him all terminology, codes, abbreviations, and the logic in arriving at any decision affecting him.

Therefore the employee was entitled to have a copy of a summarisation relating to the calculation of his bonus. He was not entitled to a copy of the rules of the bonus scheme as these were guiding principles for the use of the company and not information personally relating to the employee.

The company complied with the Commissioner's recommendation.

International Conference of Data Protection Authorities

The Commissioner and Assistant Commissioner attended the 28th International Conference of Data Protection and Privacy Commissioners, which was held in London on 2nd and 3rd November. It was attended by delegates representing 58 data protection and privacy authorities from around the world.

The main part of the Conference, at which representatives of a wide range of governmental, law enforcement, civil society and private sector organisations were also present, considered the implications of a surveillance society.

A number of themes were emphasised by Commissioners:-

- **The 'Surveillance Society' is already with us.**

Surveillance involves the purposeful, routine and systematic recording by technology of individuals' movements and activities in public and private spaces. Everyday encounters with modern and developing technology which records, sorts and sifts personal information include:

- systematic tracking, monitoring and recording of identities, movements and activities;
- analysis of spending habits, financial transactions and other interactions;
- ever-growing use of new technologies, such as automated video cameras, RFID etc;
- monitoring of telephones, e-mails and internet use; and
- monitoring of workplace activity.

- **Surveillance activities can be well-intentioned and bring benefits.**

So far the expansion of these activities has developed in relatively benign and piecemeal ways in democratic societies - not because governments or businesses necessarily wish to intrude into the lives of individuals in an unwarranted way. Some of these activities are necessary or desirable in principle - for example, to fight terrorism and serious crime, to improve entitlement and access to public services, and to improve healthcare.

- **But unseen, uncontrolled or excessive surveillance activities also pose risks that go much further than just affecting privacy.**

They can foster a climate of suspicion and undermine trust. The collection and use of vast amounts of personal information by public and private organisations leads to decisions which directly influence peoples' lives. By classifying and profiling automatically or arbitrarily, they can stigmatise in ways which create risks for individuals and affect their access to services. There is particularly an increasing risk of social exclusion.

- **Privacy and data protection regulation is an important safeguard but not the sole answer.**

The effects of surveillance on individuals do not just reduce their privacy. They also can affect their opportunities, life chances and lifestyle. Excessive surveillance also impacts on the very nature of society. Privacy and data protection rules help to keep surveillance within legitimate limits and include safeguards. However, more sophisticated approaches to regulation need to be adopted.

- **A systematic use of impact assessments should be adopted.**

Such assessments would include but be wider than privacy impact assessments, identifying social impact and opportunities for minimising undesirable consequences for individuals and society.

- **The issues are wide ranging and cannot be taken forward by data protection/privacy regulators alone.**

Engagement should be a common cause for all who are concerned about developments. Commissioners should work alongside relevant civil society organisations and also governments, private sector, elected representatives and individuals themselves to guard against unwarranted consequences.

- **Public trust and confidence is paramount.**

Although much of the infrastructure of the surveillance society has been assembled for benign purposes, continued public trust cannot be taken for granted. Individuals must feel confident that any intrusion into their lives is for necessary and proportionate purposes. Public confidence is like personal privacy - once lost it is difficult if not impossible to regain. Although surveillance society issues are broader than data protection and privacy, data protection authorities have an indispensable role to play. Increasingly in a surveillance society individuals often have no realistic choices, little control and few opportunities for self help. Personal information is collected and used in ways invisible to the ordinary individual. During the lifetime of data protection regulation the world has not stood still. The demands of states, private sector and citizens have changed and information processing technology has moved on at a fast pace. It is right for data protection authorities to reflect upon whether their traditional approaches remain relevant and effective. Activities such as complaint handling and audit/inspection are as important as ever but continued improvement in areas such as effective engagement with citizens and policy makers is now essential.

During the closed session of the Conference, the Commissioners welcomed an initiative from Alex Türk, President of the French Commission Nationale de l'Informatique et des Libertés (CNIL), urging them to re-state the fundamental importance of data protection and privacy in a fast-changing world and the need for urgent action to face new challenges. A copy of the Statement – “*Communicating Data Protection and Making It More Effective*” – together with further information about the conference, is published on the conference website: <http://www.privacyconference2006.co.uk/> .

The Commissioners reflected upon their own role and the challenges that these changes pose for them. Commissioners identified the following areas as necessary to allow them to rise to the challenges:

- **Protection of citizens' privacy and personal data is vital** for any democratic society, on the same level as freedom of the press or freedom of movement. Privacy and data protection may in fact be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.
- **Commissioners should develop a new communication strategy** in order to make the public and relevant stakeholders more aware of these rights and their importance. Commissioners should initiate powerful and long term awareness raising campaigns and measure the effects of these actions.
- **Commissioners should also communicate better** about their own activities and make data protection more concrete. Only when these activities are meaningful, accessible and relevant for the public at large, is it possible to gain the necessary power to influence public opinion and to be heard by decision makers.
- **Commissioners should assess their efficiency and effectiveness**, and where necessary adapt their practices. They should be granted sufficient powers and resources, but should also use them in a selective and pragmatic manner, while concentrating at serious and likely harms, or main risks facing individuals.
- **Commissioners should reinforce their capacities in technological areas**, with a view to advanced studies, expert opinions and interventions, in close interaction with research and industry in the field of new technology, and share this work together. The excessively "legal" image of data protection must be corrected.
- **Commissioners should restructure the International Conference** to become a stronger voice on international issues and an unavoidable discussion partner for international initiatives with an incidence on data protection.
- **Commissioners should support the need of an International Convention** and the development of other global instruments. Problems that can only be dealt with effectively at international level – either in general or in specific sectors – should be addressed in this way with appropriate means.
- **Commissioners should promote the involvement of other stakeholders** of data protection and privacy, at national or international level, such as civil society and NGOs, to develop strategic partnerships where appropriate, with a view to making their work more effective.

Commissioners agreed to undertake a programme of follow-up activities along these lines and to consider and evaluate progress made at their next international conference. In addition to considering their own role, Commissioners also adopted the following important resolutions.

- Accreditation of eight new members - the data protection authorities of: Andorra, Liechtenstein, Estonia, Romania, Gibraltar and Canada - New Brunswick, Northwest Territories and Nunavut
- A resolution on conference organisational arrangements
- A resolution prepared by the International Working Group on Data Protection in Telecommunications on: "Privacy Protection and Search Engines".

In conclusion, the challenges facing society and Data Protection and Privacy Commissioners are substantial. Not just in terms of surveillance but also due to the rapid changes in information processing technology, increased globalisation, irreversibility of some developments and lack of public awareness and education. Data protection safeguards, and the independent authorities which help set and enforce these safeguards, are indispensable in the modern information age. Commissioners have risen to the challenge and are committed to redoubling their efforts to ensure that data protection controls are even more relevant today and in the future than they were when many of today's developments were in their infancy.

European Spring Conference

The Assistant Commissioner attended the European Spring conference, which was held in Budapest on 24th and 25th April 2006. She was one of 103 delegates representing data protection authorities throughout Europe.

The conference focused on the challenges faced by data protection authorities in protecting the rights of individuals in regard to the processing of their information in the world of today.

For instance personal privacy is threatened by the increasing need for countries to exchange information in order to combat the increase in organised crime and terrorism. Data protection must not be an obstacle to this work but it is necessary to ensure that such exchanges of information are necessary and proportionate to achieve the desired aims.

Other threats to personal privacy come from innovations in technology such as Radio Frequency Identification (RFID) tags which make it possible trace the whereabouts of individuals.

Electronic health records may be perceived as a means of making health care delivery more effective and efficient but there are challenges in ensuring that they are accurate, up to date and most of all secure.

The conference discussed how data protection authorities could work together to achieve common data protection standards across jurisdictions in order to meet these challenges.

International Working Group on Data Protection in Telecommunications (IWGDPT)

The Commissioner attended the two meetings of the International Working Group that were held in 2006.

The 39th meeting was held in Washington, DC on 6th and 7th April and was preceded by an international workshop organised by the Privacy Office of the US Department of Homeland Security, entitled: "Transparency and Accountability – The Use of Personal Information within the Government".

The 40th meeting of the Working Group was held in Berlin on 5th and 6th September. Representatives from China and Romania joined the Group for the first time at this meeting, which included 59 participants from 31 countries.

Both meetings covered similar topics, mainly concerned with the production of working papers addressing the following issues:

- IP Telephony (Voice over IP)
- Voice Analysis Technology
- Privacy and Search Engines
- Trusted Computing and Digital Rights Management
- Privacy and Cross-Border Marketing
- Online Availability of Electronic Health Records
- Spam
- E-Government
- RFID
- Vehicle Event Recorders
- Personal data within WHOIS databases
- Privacy aspects of the World Summit on the Information Society

The 41st meeting of the Working Group will be held in Guernsey on 12th and 13th April 2007 and be preceded by a public conference on 11th April.

Liaison between the British, Irish and Islands' Data Protection Authorities

The Commissioner and Assistant Commissioner joined representatives from the authorities of the UK, Ireland, Jersey, Cyprus and Gibraltar, who attended the annual meeting, which was held in the Isle of Man on 4th July 2006. The Commissioner from Malta was unfortunately unable to attend.

This was the first meeting at which Gibraltar had been represented and the delegates from Gibraltar outlined the role of the Gibraltar Regulatory Authority, which encompasses a range of responsibilities, including Financial Services, Telecommunications and Data Protection.

The Commissioner summarised the main issues being discussed at the International Working Group on Data Protection in Telecommunications and the Isle of Man Supervisor introduced the topic of mandatory notification of security breaches, a practice that originated in the United States.

The Authorities also discussed the different legislative and supervisory approaches that were being adopted to the facilitation of Public Access to Official Information, otherwise known as Freedom of Information.

It is planned that the next meeting of the Authorities will be held in July 2007 in Guernsey.

Liaison with the UK Government

No meetings were held with staff from the Department of Constitutional Affairs during 2006. However, email contact with officials was maintained and the Department commenced publication of the Information Rights Journal, which provides specific information on policy and case law on Data Protection and Freedom of Information.

Data Protection Forum

The Assistant Commissioner attended three meetings of the Data Protection Forum that were held in London during 2006; the topics covered in the meetings were:

- *The development of international standards for data retention*
- *Data sharing across the public and private sectors*
- *The re-use of public sector information*
- *The work of the UK Information Tribunal*
- *The role and responsibilities of the UK Passport Agency*
- *Perspectives from data protection authorities in the UK, Ireland and Crown Dependencies*
- *Developments in European data protection*
- *Review of data protection issues during 2006*

It is considered that attendance at these meetings provides benefits which include:

- networking with key people involved in data protection, in many cases from parent companies with offices in Guernsey ;
- the opportunity to influence data protection policy-making;
- raising the awareness of pertinent issues and future trends that may affect both the public and private sectors.

Information Privacy Expert Panel

The Commissioner attended the three meetings of the British Computer Society [BCS] Information Privacy Expert Panel [IPEP], which were held in London during the year.

The IPEP includes members from academia, the public and private sectors and has considered various topics, including the UK Government proposals on Identity Cards and data sharing initiatives within the public sector.

The cost of attendance at these quarterly meetings of the IPEP and at any related meetings is borne by the BCS. Another positive outcome of this involvement has been the substantial sponsorship of the 2007 conference that was secured from the BCS.

OBJECTIVES FOR 2007

The primary objectives for 2007 will encompass the following areas:-

- ***Legislation***

Detailed work on the amendments to the Data Protection legislation will continue.

- ***Adequacy and International Transfers***

Work will continue to ensure that the European Commission's adequacy finding for the Data Protection régime in the Bailiwick is respected and that international data transfers comply with the eighth Data Protection principle.

- ***British Isles and International Liaison***

Work will concentrate on the organisation of the conference "Respecting Privacy in Global Networks" to be held in Guernsey on 11th April, the arrangements for the 41st meeting of the International Working Group on Data Protection in Telecommunications on 12th and 13th April and the meeting of the British Isles and Islands' meeting to be held on 12th July.

Participation in relevant UK, European and international conferences will continue as a means of enhancing the international recognition of the independent status and regulatory prowess of the Bailiwick and ensuring that local knowledge of international developments remains up to date.

- ***Raising Awareness***

The media will be used to continue the awareness campaign and a further series of seminars and talks for the public and private sectors will be mounted.

Collaboration with the Training Agency will continue over the organisation of courses leading to formal qualifications in data protection, such as the ISEB Certificate.

Promotion of relevant training using UK specialists will be done, with training being targeted separately to financial sector organisations, other private sector organisations and the public sector.

The publication of new literature and the review and revision of existing literature will be undertaken as the need arises.

Promotion of the Telephone and Fax Preference Services and periodic surveys to determine their use and effectiveness will be undertaken.

- ***Compliance***

Targeted compliance activities will be organised to increase the notification level of local organisations. More rigorous enforcement will take place, including consideration of prosecution of non-compliant organisations.

The monitoring of websites and periodic surveys to assess compliance with data protection legislation and the privacy regulations will be done.

- ***Government***

Close liaison with the States of Guernsey Government departments will continue with the aim of promoting data sharing protocols and the further development of subject access procedures.

FINANCIAL REPORT

The Data Protection Office is funded by a grant from the States of Guernsey that is administered by the Home Department. This grant is based on a budgetary estimate of expenditure prepared annually by the Commissioner.

In accordance with Section 3 of Schedule 5 of the Law, all fees received are repaid into the General Revenue Account.

The Data Protection Office's Income and Expenditure, which are included within the published accounts for the Home Department, have been as follows:

<u>INCOME</u>	2006	2005
	£	£
Data Protection Fees ¹	43,382	41,686
<u>EXPENDITURE</u>		
Rent	15,526	16,276
Salaries and Allowances ²	138,328	137,251
Travel and Subsistence	10,588	9,751
Furniture and Equipment	13,806	14,237
Publications	2,886	2,609
Post, Stationery, Telephone	3,542	4,253
Heat Light, Cleaning	4,743	4,874
TOTAL EXPENDITURE	£189,419	£189,251
EXCESS OF EXPENDITURE OVER INCOME	<u>£146,037</u>	<u>£147,565</u>

NOTES

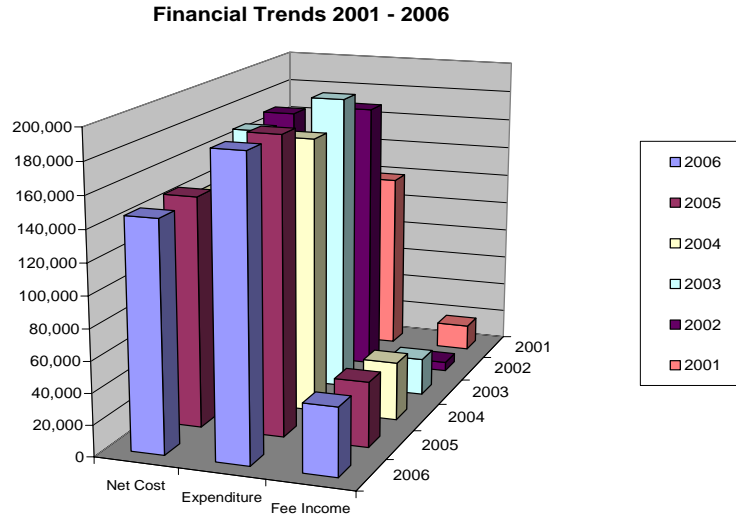
¹ Fees were £35 per notification or renewal of a notification.

Income from fees is accrued on a monthly basis.

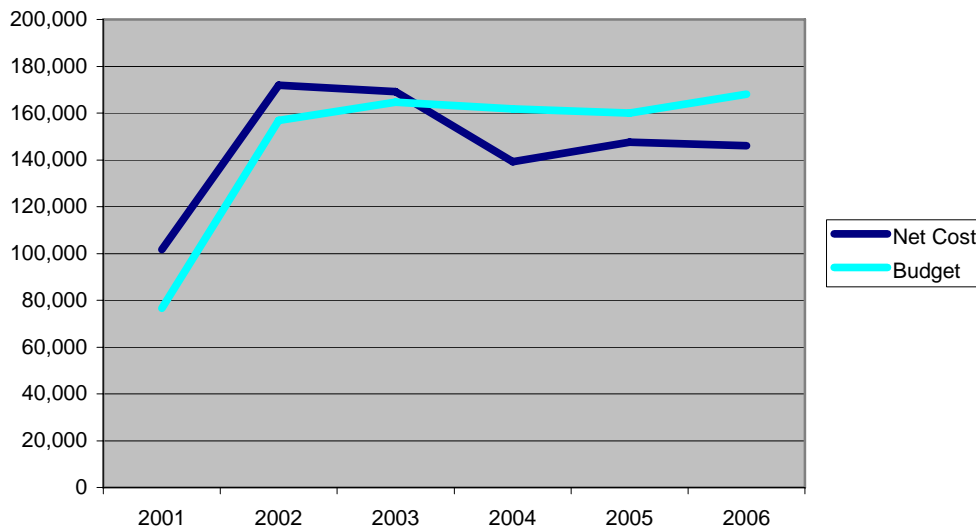
The cash received for notifications in 2006 was £43,505 (£42,665 in 2005) representing the 1,243 annual notifications and renewals that were processed during 2006.

² This includes an amount of £1,662 (£6,270 in 2005) for consultancy fees.

The financial trends in income and expenditure since 2001 are shown graphically below.



Net cost vs budget 2001 - 2006



Expenditure for 2006 was held at the same level as 2005 and a small increase in the income from fees enabled the net cost of the Office to be reduced and to remain below the authorised budget for the third year running. It is anticipated that the increase in Notification Fees which has been approved by the States would bring in an additional £17,000 of income in a full year, enabling the net cost of the Office to be reduced further.

It is confirmed that no gifts or hospitality were received by the Commissioner or his staff during 2006.

APPENDIX

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and special conditions apply to the processing of sensitive personal data.
2. Personal data shall be obtained for one or more specified and lawful purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed.
4. Personal data shall be accurate and kept up to date.
5. Personal data shall not be kept for longer than necessary.
6. Personal data shall be processed in accordance with the rights of data subjects.
7. Technical and organisational measures shall be taken against unauthorised or unlawful processing and against accidental loss or damage to personal data.
8. Personal data shall not be transferred to a country or territory outside the Bailiwick unless the destination ensures an adequate level of protection for the data.

THE PRIVACY AND ELECTRONIC COMMUNICATIONS REGULATIONS

1. Telecommunications services must be secure and information processed within such services must be kept confidential.
2. Traffic data should not be retained for longer than necessary and the detail of itemised billing should be under subscriber control.
3. Facilities should be provided for the suppression of calling line and connected line information.
4. Information on the subscriber's location should not generally be processed without consent.
5. Subscribers may choose not to appear in directories.
6. Automated calling systems may not be used for direct marketing to subscribers who have opted out.
7. Unsolicited faxes may not be sent to private subscribers unless they have opted in or to business subscribers who have opted out.
8. Unsolicited marketing calls may not be made to subscribers who have opted out.
9. Unsolicited email marketing may not be sent to private subscribers and must never be sent where the identity of the sender has been disguised or concealed.
10. The Data Protection Commissioner may use enforcement powers to deal with any alleged contraventions of the Regulations.

Further information about compliance with the Data Protection (Bailiwick of Guernsey) Law 2001 can be obtained via:

E-mail address: dataprotection@gov.gg
Internet: www.gov.gg/dataprotection
Telephone: +44 (0) 1481 742074
Fax: +44 (0) 1481 742077



Post: Data Protection Commissioner's Office
P.O. Box 642
Frances House
Sir William Place
St. Peter Port
Guernsey
GY1 3JE